

Configuración de RTP seguro en Contact Center Enterprise

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Tarea 1: Configuración segura de CUBE](#)

[Tarea 2: Configuración segura de CVP](#)

[Tarea 3: Configuración segura de CVB](#)

[Tarea 4: Configuración segura de CUCM](#)

[Establecer el modo de seguridad de CUCM en modo mixto](#)

[Configuración de los perfiles de seguridad del troncal SIP para CUBE y CVP](#)

[Asociar perfiles de seguridad de línea troncal SIP a líneas troncales SIP respectivas y habilitar SRTP](#)

[Comunicación de dispositivos de agentes seguros con CUCM](#)

[Verificación](#)

Introducción

En este documento se describe cómo proteger el tráfico del protocolo de transporte en tiempo real (SRTP) en el flujo de llamadas completo de Contact Center Enterprise (CCE).

Prerequisites

La generación e importación de certificados no están incluidas en el ámbito de este documento, por lo que se deben crear e importar certificados para Cisco Unified Communication Manager (CUCM), el servidor de llamadas del portal de voz del cliente (CVP), Cisco Virtual Voice Browser (CVVB) y Cisco Unified Border Element (CUBE) en los componentes respectivos. Si utiliza certificados autofirmados, el intercambio de certificados debe realizarse entre los diferentes componentes.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- CCE
- CVP
- CUBO
- CUCM
- CVVB

Componentes Utilizados

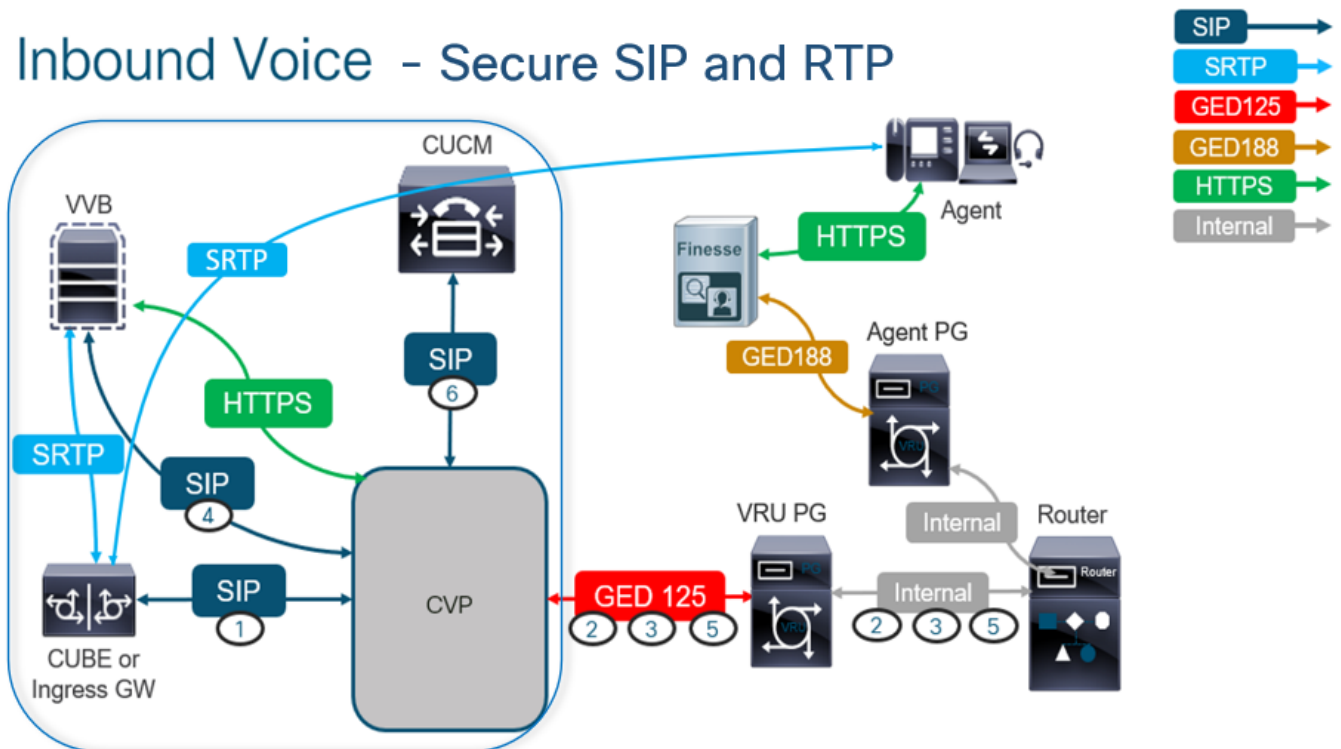
La información de este documento se basa en Package Contact Center Enterprise (PCCE), CVP, CVB y CUCM versión 12.6, pero también es aplicable a las versiones anteriores.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Nota: en el flujo de llamadas completo del centro de contacto, para habilitar RTP seguro, deben habilitarse las señales SIP seguras. Por lo tanto, las configuraciones en este documento habilitan tanto el SIP seguro como el SRTP.

El siguiente diagrama muestra los componentes implicados en las señales SIP y RTP en el flujo de llamadas completo del centro de contacto. Cuando el sistema recibe una llamada de voz, primero se realiza a través del gateway de entrada o CUBE, por lo que debe iniciar las configuraciones en CUBE. A continuación, configure CVP, CVB y CUCM.



Tarea 1: Configuración segura de CUBE

En esta tarea, configure CUBE para proteger los mensajes del protocolo SIP y RTP.

Configuraciones necesarias:

- Configuración de un punto de confianza predeterminado para SIP UA
- Modificar los pares de marcado para utilizar TLS y SRTP

Pasos:

1. Abra una sesión SSH en CUBE.
2. Ejecute estos comandos para que la pila SIP utilice el certificado CA del CUBE. CUBE establece una conexión SIP TLS desde/hacia CUCM (198.18.133.3) y CVP (198.18.133.13):

```
Conf t Sip-ua Transport tcp tls v1.2 crypto signaling remote-addr 198.18.133.3 255.255.255.255 trustpoint ms-ca-name crypto signaling remote-addr 198.18.133.13 255.255.255.255 trustpoint ms-ca-name exit
```

```
CC-VCUBE (config)#sip-ua
CC-VCUBE (config-sip-ua)#transport tcp tls v1.2
CC-VCUBE (config-sip-ua)#crypto signaling remote-addr 198.18.133.3 255.255.255.255 trustpoint ms-ca-name
CC-VCUBE (config-sip-ua)#crypto signaling remote-addr 198.18.133.13 255.255.255.255 trustpoint ms-ca-name
CC-VCUBE (config-sip-ua)#exit
CC-VCUBE (config)#
```

3. Ejecute estos comandos para habilitar TLS en el par de marcado saliente para CVP. En este ejemplo, la etiqueta dial-peer 6000 se utiliza para rutear llamadas a CVP:

```
Conf t dial-peer voice 6000 voip session target ipv4:198.18.133.13:5061 session transport tcp tls srtp exit
```

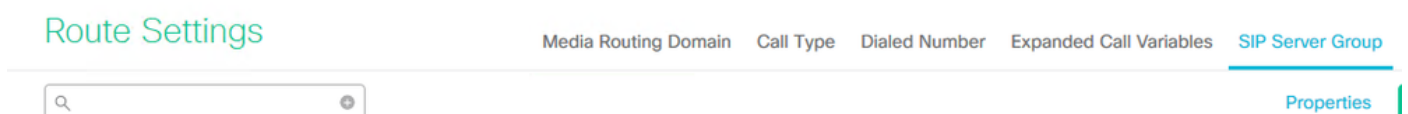
```
CC-VCUBE#
CC-VCUBE#Conf t
Enter configuration commands, one per line. End with CNTL/Z.
CC-VCUBE (config)#dial-peer voice 6000 voip
CC-VCUBE (config-dial-peer)#session target ipv4:198.18.133.13:5061
CC-VCUBE (config-dial-peer)#session transport tcp tls
CC-VCUBE (config-dial-peer)#SRTP
CC-VCUBE (config-dial-peer)#exit
CC-VCUBE (config)#
CC-VCUBE (config)#
```

Tarea 2: Configuración segura de CVP

En esta tarea, configure el servidor de llamadas CVP para proteger los mensajes del protocolo SIP (SIP TLS).

Pasos:

1. Inicie sesión en el UCCE Web Administration.
2. Desplácese hasta Call Settings > Route Settings > SIP Server Group.



Según sus configuraciones, tiene grupos de servidores SIP configurados para CUCM, CVB y CUBE. Debe establecer los puertos SIP seguros en 5061 para todos ellos. En este ejemplo, se utilizan estos grupos de servidores SIP:

- cucm1.dcloud.cisco.com para CUCM

- vvb1.dcloud.cisco.com para CVVB
- cube1.dcloud.cisco.com para CUBE

3. Haga clic en `cucm1.dcloud.cisco.com`, a continuación, en el **Members** que muestra los detalles de las configuraciones de grupos de servidores SIP. Set SecurePort a 5061 y haga clic en Save.

Route Settings [Media Routing Domain](#) [Call Type](#) [Dialed Number](#) [Expanded Call Variables](#) **Sip Server Groups** [Routing Pattern](#)

Edit cucm1.dcloud.cisco.com

General **Members**

List of Group Members +

Hostname/IP	Priority	Weight	Port	SecurePort	Site
198.18.133.3	10	10	5060	5061	Main

4. Haga clic en `vvb1.dcloud.cisco.com` y luego en el **Members**, establezca la ficha **SecurePort** a 5061 y haga clic en Save.

Route Settings [Media Routing Domain](#) [Call Type](#) [Dialed Number](#) [Expanded Call Variables](#) **Sip Server Groups**

Edit vvb1.dcloud.cisco.com

General **Members**

List of Group Members +

Hostname/IP	Priority	Weight	Port	SecurePort	Site
vvb1.dcloud.cisco.c...	10	10	5060	5061	Main

Tarea 3: Configuración segura de CVB

En esta tarea, configure CVB para proteger los mensajes de protocolo SIP (SIP TLS) y SRTP.

Pasos:

1. Abra el Cisco VVB Admin página.
2. Desplácese hasta `System > System Parameters`.



Cisco Virtualized Voice Browser Administration

For Cisco Unified Communications Solutions

System Applications Subsystems Tools Help

System Parameters

Logout

Cisco Virtualized Voice Browser Administration

System version: 12.5.1.10000-24

3. En el Security Parameters sección, elija Enable para TLS (SIP) . Guarde el Supported TLS(SIP) version as TLSv1.2 y elija Enable para SRTP.

Parameter Name	Parameter Value	Suggested Value
TLS(SIP)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	Disable
Supported TLS(SIP) Versions	TLSv1.2	TLSv1.2
▶ Cipher Configuration		TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
SRTP <small>[Crypto Suite : AES_CM_128_HMAC_SHA1_32]</small>	<input type="radio"/> Disable <input checked="" type="radio"/> Enable <input type="checkbox"/> Allow RTP (Mixed mode)	Disable

4. Haga clic en Update. Haga clic en ok cuando se le solicite que reinicie el motor CVB.

The screenshot shows the 'System Parameters Configuration' page with an 'Update' button. A dialog box is displayed over the page, containing the text: 'vwb1.dcloud.cisco.com says Please restart Cisco VVB Engine for the updates to take effect.' and an 'OK' button.

5. Estos cambios requieren que se reinicie el motor Cisco VB. Para reiniciar el motor VB, navegue hasta el Cisco VVB Serviceability , haga clic en Go.

The screenshot shows the 'Navigation' menu with the following options: 'Cisco VVB Administration', 'Cisco VVB Administration', 'Cisco Unified Serviceability', 'Cisco VVB Serviceability', and 'Cisco Unified OS Administration'. The 'Go' button is visible next to the first two options.

6. Desplácese hasta Tools > Control Center – Network Services.

The screenshot shows the 'Tools' menu with the following options: 'Control Center - Network Services' and 'Performance Configuration and Logging'.

7. Elegir Engine y haga clic en Restart.

Control Center - Network Services

Start Stop **Restart** Refresh

Status

i Ready

Select Server

Server *

System Services	
	Service Name
<input type="radio"/>	Perfmon Counter Service
<input type="radio"/>	▼Cluster View Daemon
	▶Manager Manager
<input checked="" type="radio"/>	▼Engine
	▶Manager Manager
	▶Subsystem Manager

Tarea 4: Configuración segura de CUCM

Para proteger los mensajes SIP y RTP en CUCM, realice estas configuraciones:

- Establecer el modo de seguridad de CUCM en modo mixto
- Configuración de los perfiles de seguridad del troncal SIP para CUBE y CVP
- Asociar perfiles de seguridad de línea troncal SIP a líneas troncales SIP respectivas y habilitar SRTP
- Comunicación de dispositivos de agentes seguros con CUCM

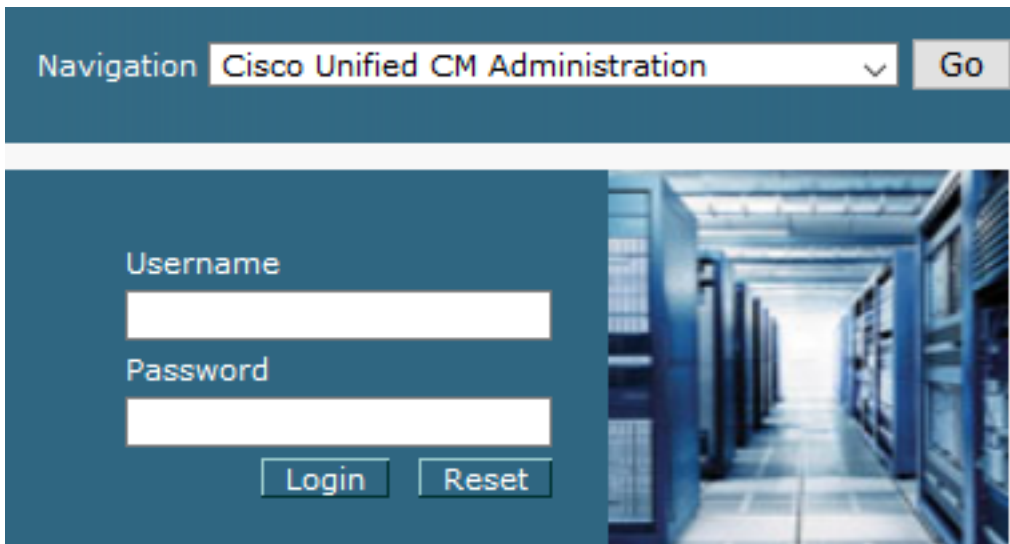
Establecer el modo de seguridad de CUCM en modo mixto

CUCM admite dos modos de seguridad:

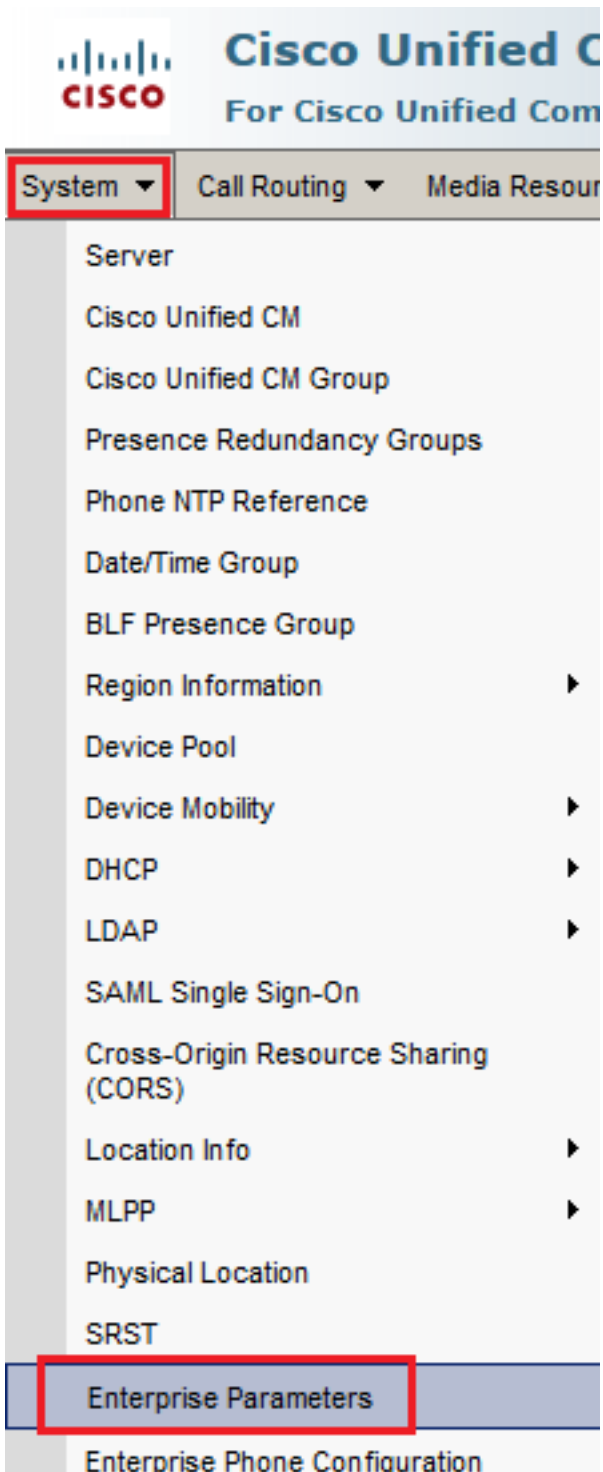
- Modo no seguro (modo predeterminado)
- Modo mixto (modo seguro)

Pasos:

1. Inicie sesión en la interfaz de administración de CUCM.



2. Al iniciar sesión en CUCM, puede navegar hasta **System > Enterprise Parameters**.



3. En la sección Security Parameters sección, compruebe si el Cluster Security Mode se establece en 0.



4. Si el modo de seguridad de clúster está establecido en 0, significa que el modo de seguridad de clúster está establecido en no seguro. Debe habilitar el modo mixto desde CLI.

5. Abra una sesión SSH en CUCM.

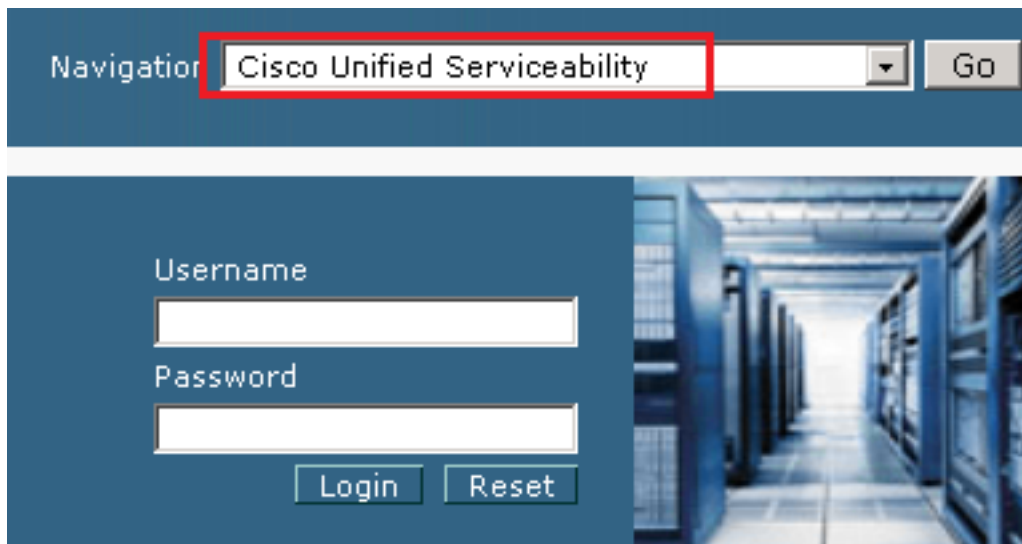
6. Tras iniciar sesión correctamente en CUCM a través de SSH, ejecute este comando:

```
utils ctl set-cluster xed-mode
```

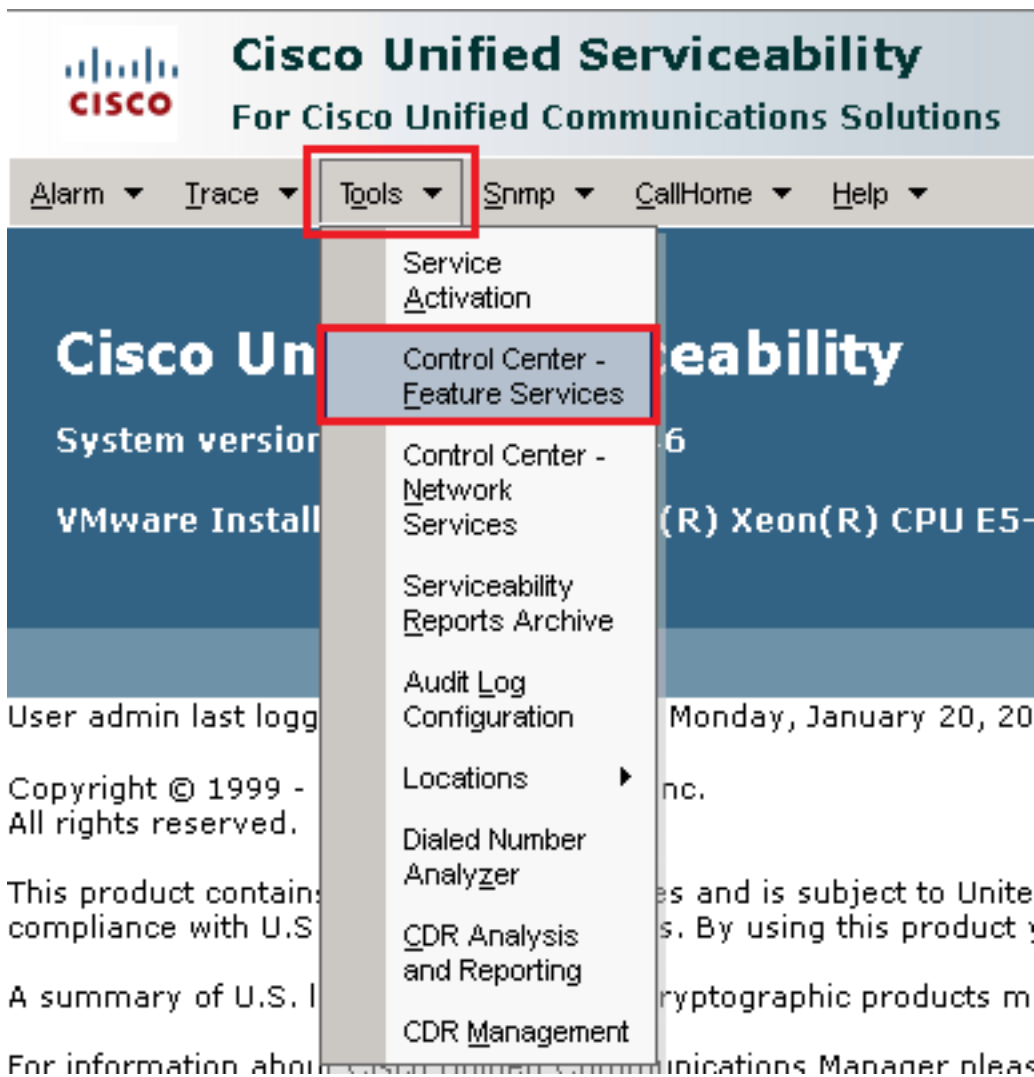

7. Tipo `y` y haga clic en `Enter` cuando se lo solicite. Este comando establece el modo de seguridad del clúster en modo mixto.

```
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n): y
Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
Please restart Cisco CallManager service and Cisco CTIManager services on all the nodes in the cluster that run these services.
admin:
```

- 8. Para que los cambios surtan efecto, reinicie el Cisco CallManager y el Cisco CTIManager servicios.
- 9. Para reiniciar los servicios, navegue e inicie sesión en Cisco Unified Serviceability.



10. Después de iniciar sesión correctamente, vaya a `Tools > Control Center – Feature Services`.



11. Elija el servidor y haga clic en Go.



12. Debajo de los servicios de CM, seleccione el Cisco CallManager , haga clic en Restart situado en la parte superior de la página.

CM Services	
	Service Name
<input checked="" type="radio"/>	Cisco CallManager
<input type="radio"/>	Cisco Unified Mobile Voice Access Service
<input type="radio"/>	Cisco IP Voice Media Streaming App
<input type="radio"/>	Cisco CTIManager
<input type="radio"/>	Cisco Extension Mobility

13. Confirme el mensaje emergente y haga clic en **OK**. Espere a que el servicio se reinicie correctamente.

Restarting Service. It may take a while... Please wait for the page to refresh.
If you see Starting/Stopping state, refresh the page after sometime to show the right status.



14. Después del reinicio correcto de Cisco CallManager, seleccione la **Cisco CTIManager** haga clic en **Restart** botón para reiniciar **Cisco CTIManager** servicio.

CM Services	
	Service Name
<input type="radio"/>	Cisco CallManager
<input type="radio"/>	Cisco Unified Mobile Voice Access Service
<input type="radio"/>	Cisco IP Voice Media Streaming App
<input checked="" type="radio"/>	Cisco CTIManager
<input type="radio"/>	Cisco Extension Mobility

15. Confirme el mensaje emergente y haga clic en **OK**. Espere a que el servicio se reinicie correctamente.

Restarting Service. It may take a while... Please wait for the page to refresh.
If you see Starting/Stopping state, refresh the page after sometime to show the right status.



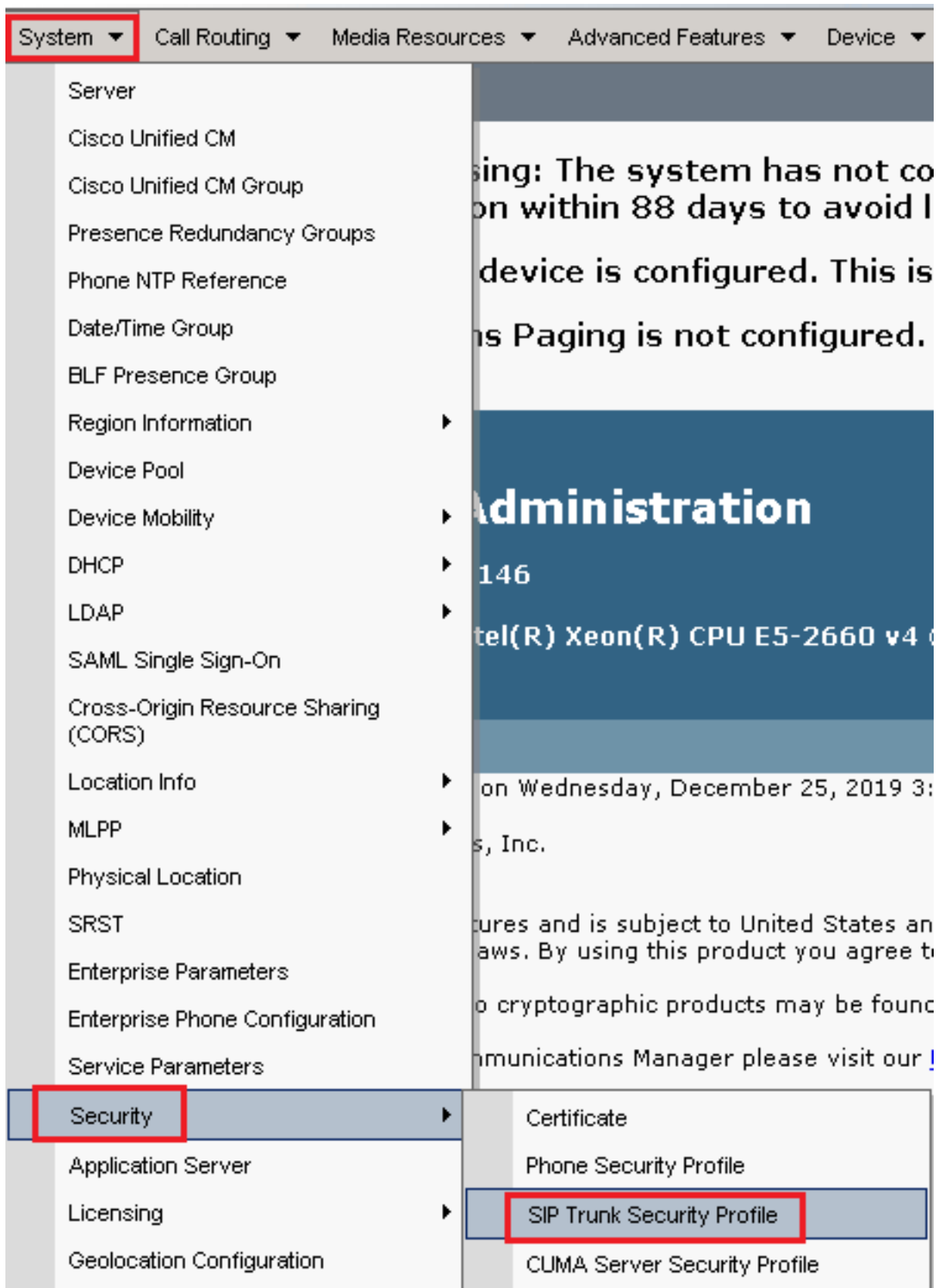
16. Después de reiniciar correctamente los servicios, para verificar que el modo de seguridad del clúster está configurado en modo mixto, navegue hasta la administración de CUCM como se explicó en el paso 5 y, a continuación, verifique la **Cluster Security Mode**. Ahora debe configurarse en **1**.

Security Parameters	
Cluster Security Mode *	1
Cluster SIPOAuth Mode *	Disabled

Configuración de los perfiles de seguridad del troncal SIP para CUBE y CVP

Pasos:

1. Inicie sesión en la interfaz de administración de CUCM.
2. Después de iniciar sesión correctamente en CUCM, vaya a **System > Security > SIP Trunk Security Profile** para crear un perfil de seguridad de dispositivo para CUBE.



3. En la parte superior izquierda, haga clic en **Add New** para agregar un nuevo perfil.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features







Find and List SIP Trunk Security Profiles

 Add New  Select All  Clear All  Delete Selected



4. Configurar SIP Trunk Security Profile como esta imagen y haga clic en Save en la parte inferior izquierda de la página.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk A

SIP Trunk Security Profile Configuration Related Links: [Back](#)

 Save  Delete  Copy  Reset  Apply Config  Add New

- Status -

-  Add successful
-  Reset of the trunk is required to have changes take effect.

- SIP Trunk Security Profile Information -

Name*	SecureSIPTLSforCube
Description	
Device Security Mode	Encrypted ▾
Incoming Transport Type*	TLS ▾
Outgoing Transport Type	TLS ▾
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
Secure Certificate Subject or Subject Alternate Name	SIP-GW
Incoming Port*	5061
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input type="checkbox"/> Accept unsolicited notification	
<input type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter ▾

5. Asegúrese de establecer el **Secure Certificate Subject or Subject Alternate Name** al nombre común (CN) del certificado de CUBE, ya que debe coincidir.

6. Haga clic **Copy** y cambiar el **Name** a **SecureSipTLSforCVP**. Cambiar **Secure Certificate Subject** al CN del certificado del servidor de llamadas CVP, ya que debe coincidir. Haga clic en **save** botón.

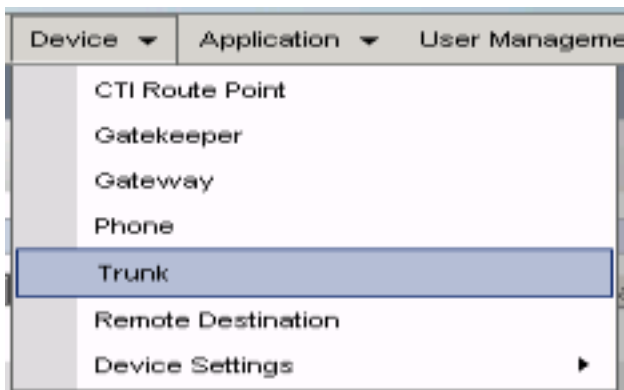
The screenshot displays the configuration page for a SIP Trunk Security Profile. At the top, there is a toolbar with icons for Save, Delete, Copy, Reset, Apply Config, and Add New. Below the toolbar, the **Status** section shows two messages: "Add successful" and "Reset of the trunk is required to have changes take effect." The main section is titled **SIP Trunk Security Profile Information**. It contains several fields and options:

- Name***: SecureSIPTLSforCvp
- Description**: (empty)
- Device Security Mode**: Encrypted
- Incoming Transport Type***: TLS
- Outgoing Transport Type**: TLS
- Enable Digest Authentication
- Nonce Validity Time (mins)***: 600
- Secure Certificate Subject or Subject Alternate Name**: cvp1.dcloud.cisco.com
- Incoming Port***: 5061
- Enable Application level authorization
- Accept presence subscription
- Accept out-of-dialog refer**
- Accept unsolicited notification
- Accept replaces header
- Transmit security status
- Allow charging header
- SIP V.150 Outbound SDP Offer Filtering***: Use Default Filter

Asociar perfiles de seguridad de línea troncal SIP a líneas troncales SIP respectivas y habilitar SRTP

Pasos:

1. En la página Administración de CUCM, desplácese hasta **Device > Trunk**.



2. Busque el troncal CUBE. En este ejemplo, el nombre de troncal de CUBE es vCube , haga clic en Find.

Trunks (1 - 5 of 5)						
Find Trunks where Device Name begins with vCube						
	Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	cloudcherry.sip.twilio.com	dCloud_PT
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	7800	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	6016	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	7019	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_CSS	dCloud_DP	44413XX	Robot Agent Remote Destinations

3. Haga clic en vCUBE para abrir la página de configuración del troncal de vCUBE.

4. IN Device Information , compruebe la sección SRTP Allowed para habilitar el SRTP.

Unattended Port

SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information. Consider Traffic on This Trunk Secure*

Route Class Signaling Enabled* When using both sRTP and TLS

Use Trusted Relay Point* Default

5. Desplácese hacia abajo hasta el SIP Information y cambiar la sección Destination Port a 5061.

6. Cambiar SIP Trunk Security Profile a SecureSIPTLSForCube.

SIP Information

Destination

Destination Address is an SRV

1* Destination Address: 198.18.133.226 Destination Address IPv6: Destination Port: 5061

MTP Preferred Originating Codec*: 711ulaw

BLF Presence Group*: Standard Presence group

SIP Trunk Security Profile*: SecureSIPTLSforCube

Rerouting Calling Search Space: < None >

7. Haga clic en save luego Rest a save y aplicar cambios.

Trunk Configuration



Save



Delete



Reset



Add New

Status



Update successful

The configuration changes will not take effect on the trunk until a reset is performed. Use the Reset button or Job Scheduler to execute the reset.

OK

8. Desplácese hasta **Device > Trunk**, busque el troncal de CVP; en este ejemplo, el nombre del troncal de CVP es **cvp-SIP-Trunk**. Haga clic en **Find**.

Trunks (1 - 1 of 1)				
Find Trunks where				
	Device Name	begins with	cvp	Find
	Clear Filter			
	Select item or enter search text			
<input type="checkbox"/>	Name ^	Description	Calling Search Space	Device Pool
<input type="checkbox"/>	CVP-SIP-Trunk	CVP-SIP-Trunk	dCloud_CSS	dCloud_DP

9. Haga clic en **CVP-SIP-Trunk** para abrir la página de configuración del troncal de CVP.

10. IN **Device Information** sección, comprobar **SRTP Allowed** para habilitar el SRTP.

Unattended Port

SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.

Consider Traffic on This Trunk Secure* When using both sRTP and TLS

Route Class Signaling Enabled* Default

Use Trusted Relay Point* Default

11. Desplácese hacia abajo hasta el **SIP Information** sección, cambie el **Destination Port** a **5061**.

12. Cambiar **SIP Trunk Security Profile** a **SecureSIPTLSForCvp**.

SIP Information

Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 198.18.133.13		5061

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* SecureSIPTLSforCvp

13. Haga clic en **Save** luego **Rest** a save y aplicar cambios.

The configuration changes will not take effect on the trunk until a reset is performed. Use the Reset button or Job Scheduler to execute the reset.

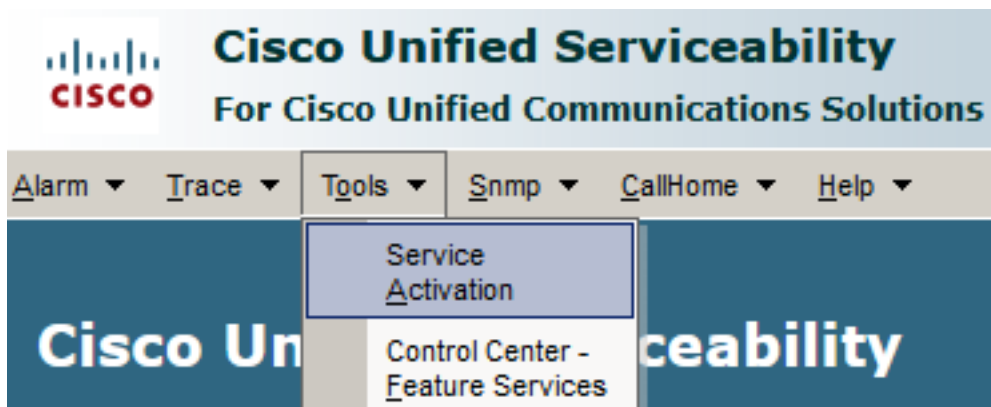
OK

Comunicación de dispositivos de agentes seguros con CUCM

Para habilitar las funciones de seguridad para un dispositivo, debe instalar un certificado de importancia local (LSC) y asignar el perfil de seguridad a ese dispositivo. El LSC posee la clave pública para el terminal, que está firmada por la clave privada CAPF de CUCM. No está instalado en los teléfonos de forma predeterminada.

Pasos:

1. Inicie sesión en Cisco Unified Serviceability interfaz.
2. Desplácese hasta Tools > Service Activation.



3. Elija el servidor de CUCM y haga clic en Go.

Service Activation

Select Server

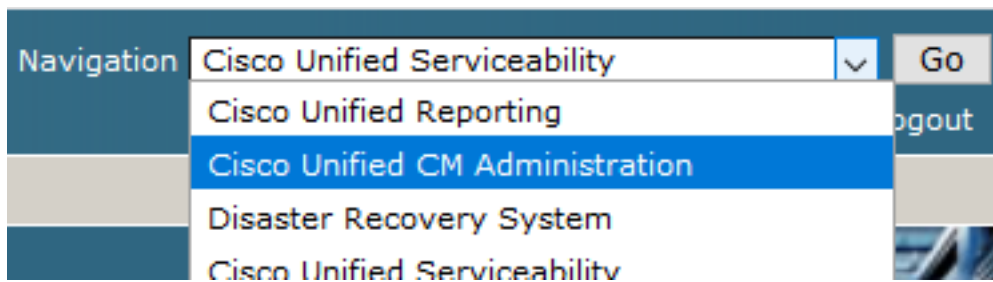
Server*

4. Cheque Cisco Certificate Authority Proxy Function y haga clic en Save para activar el servicio. Haga clic en Ok para confirmar.

Security Services

	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco Certificate Authority Proxy Function	Deactivated
<input type="checkbox"/>	Cisco Certificate Enrollment Service	Deactivated

5. Asegúrese de que el servicio está activado y, a continuación, acceda a Administración de CUCM.



6. Después de iniciar sesión correctamente en la administración de CUCM, vaya a `System > Security > Phone Security Profile` para crear un perfil de seguridad de dispositivo para el dispositivo del agente.



Cisco Unified CM Administration

For Cisco Unified Communications Solutions

System ▾

Call Routing ▾

Media Resources ▾

Advanced Features ▾

Devi

Server

Cisco Unified CM

Cisco Unified CM Group

Presence Redundancy Groups

Phone NTP Reference

Date/Time Group

BLF Presence Group

Region Information ▶

Device Pool

Device Mobility ▶

DHCP ▶

LDAP ▶

SAML Single Sign-On

Cross-Origin Resource Sharing (CORS)

Location Info ▶

MLPP ▶

Physical Location

SRST

Enterprise Parameters

Enterprise Phone Configuration

Service Parameters

Security ▶

Application Server

Licensing ▶

Geolocation Configuration

device is configured. The
as Paging is not configur

Administration

7

tel(R) Xeon(R) CPU E5-2660

on Friday, December 20, 2019 10
s, Inc.

ures and is subject to United Stat
aws. By using this product you ac

o cryptographic products may be

munications Manager please visit


our [Technical Support](#) web site.

Certificate

Phone Security Profile

SIP Trunk Security Profile

CUMA Server Security Profile

7. Busque el perfil de seguridad correspondiente a su tipo de dispositivo de agente. En este ejemplo, se utiliza un teléfono basado en software, así que elija Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile. Haga clic en icono de copia  para copiar este perfil.

Phone Security Profile (1 - 1 of 1)		Rows per Page 50
Find Phone Security Profile where	Name contains client	Find Clear Filter + -
Name	Description	Copy
Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile	Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile	

8. Cambie el nombre del perfil a Cisco Unified Client Services Framework - Secure Profile. CCambie los parámetros como en esta imagen y haga clic en Save en la parte superior izquierda de la página.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User

Phone Security Profile Configuration

Save
 Delete
 Copy
 Reset
 Apply Config
 Add New

Status

Add successful

Phone Security Profile Information

Product Type: Cisco Unified Client Services Framework
Device Protocol: SIP

Name* Cisco Unified Client Services Framework - Secure Profile
Description Cisco Unified Client Services Framework - Secure Profile
Device Security Mode Encrypted ▾
Transport Type* TLS ▾
 TFTP Encrypted Config
 Enable OAuth Authentication

Phone Security Profile CAPF Information

Authentication Mode* By Null String ▾
Key Order* RSA Only ▾
RSA Key Size (Bits)* 2048 ▾
EC Key Size (Bits) < None > ▾

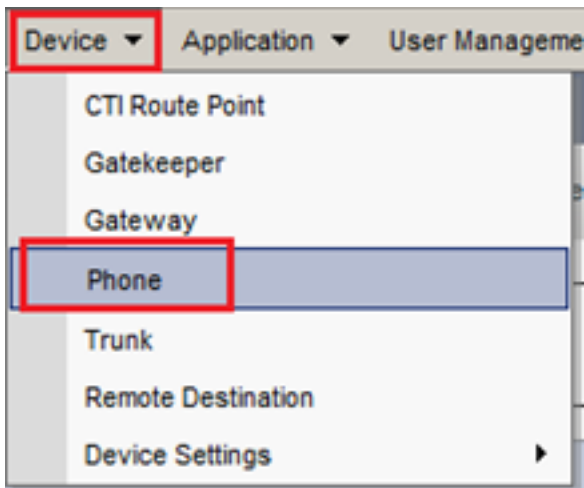
Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Parameters used in Phone

SIP Phone Port* 5061

Save Delete Copy Reset Apply Config Add New

9. Después de crear correctamente el perfil de dispositivo de teléfono, vaya a Device > Phone.



10. Haga clic en `Find` para mostrar todos los teléfonos disponibles, haga clic en teléfono del agente.
11. Se abre la página Configuración del teléfono del agente. Buscar `Certification Authority Proxy Function (CAPF) Information` sección. Para instalar LSC, configure `Certificate Operation` a `Install/Upgrade` y `Operation Completes by` en cualquier fecha futura.

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	Install/Upgrade
Authentication Mode*	By Null String
Authentication String	<input type="text"/>
<input type="button" value="Generate String"/>	
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	<input type="text"/>
Operation Completes By	2021 04 16 12 (YYYY:MM:DD:HH)

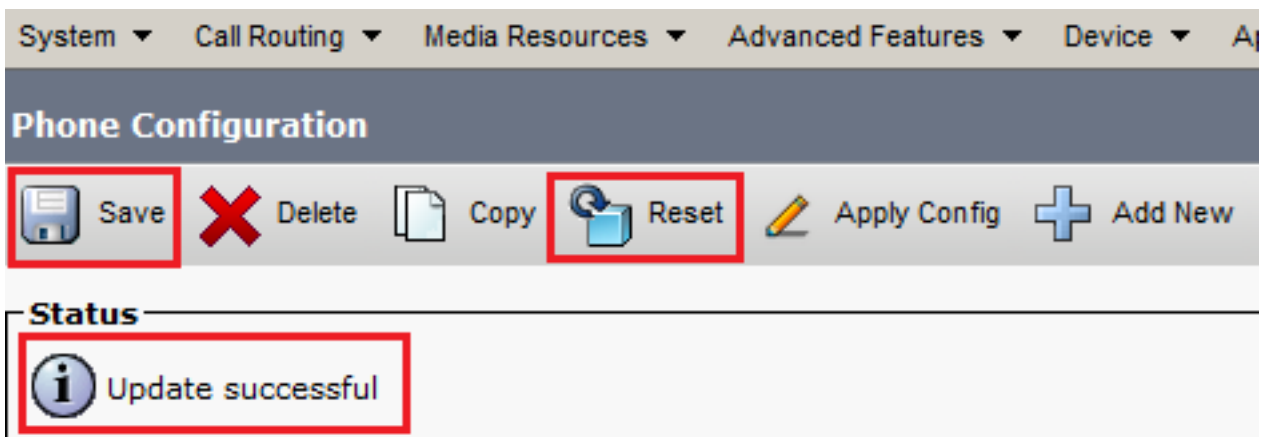
Certificate Operation Status: None
 Note: Security Profile Contains Addition CAPF Settings.

12. Buscar `Protocol Specific Information` y cambiar el `Device Security Profile` a `Cisco Unified Client Services Framework - Secure Profile`.

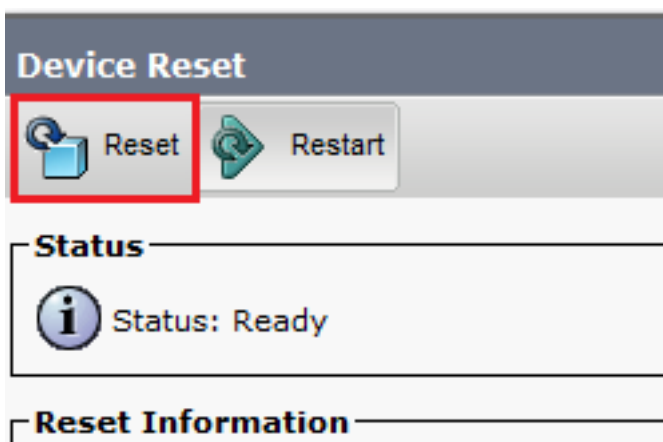
Protocol Specific Information

Packet Capture Mode*	None
Packet Capture Duration	0
BLF Presence Group*	Standard Presence group
SIP Dial Rules	< None >
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Cisco Unified Client Services Framework - Secure F
Rerouting Calling Search Space	Cisco Unified Client Services Framework - Secure Profile

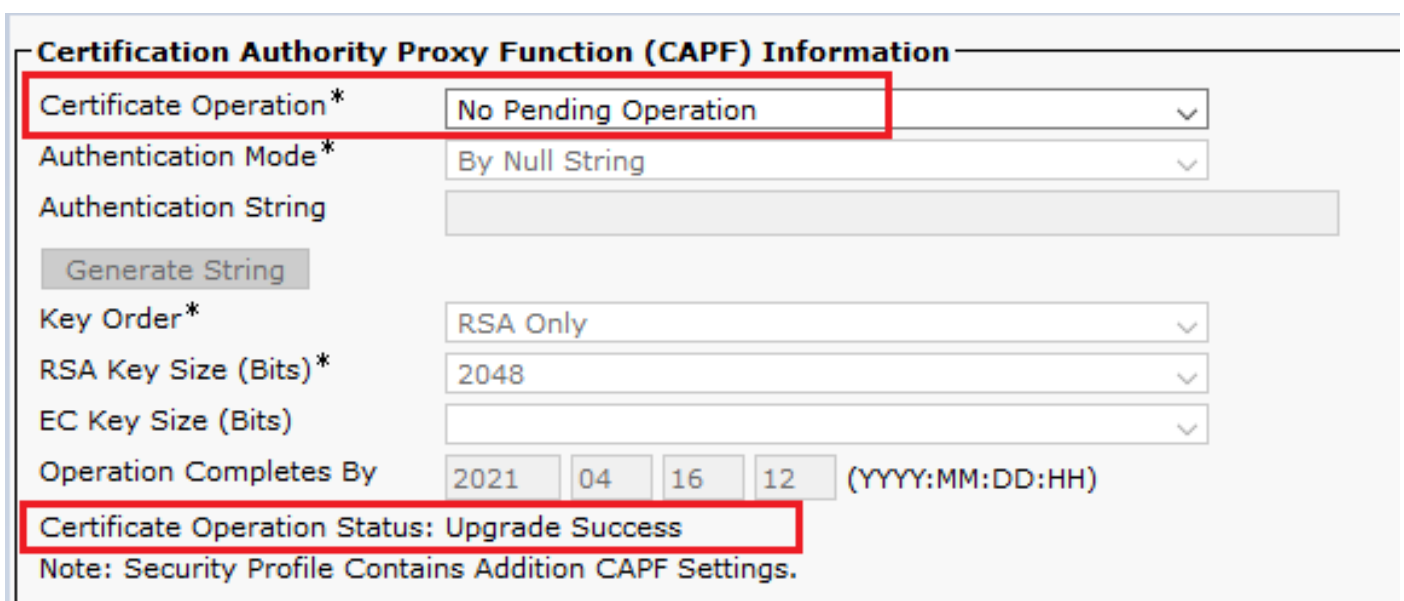
13. Haga clic en `save` en la parte superior izquierda de la página. Asegúrese de que los cambios se han guardado correctamente y haga clic en `Reset`.



14. Se abre una ventana emergente, haga clic en **Reset** para confirmar la acción.



15. Una vez que el dispositivo agente se registre de nuevo en CUCM, actualice la página actual y verifique que el LSC se haya instalado correctamente. Cheque **Certification Authority Proxy Function (CAPF) Information** sección, **Certificate Operation** se debe establecer en **No Pending Operation** y **Certificate Operation Status** se establece en **Upgrade Success**.



16. Consulte los mismos pasos en el paso 1. 7 - 13 para proteger los dispositivos de otros agentes que desea utilizar SIP y RTP seguros con CUCM.

Verificación

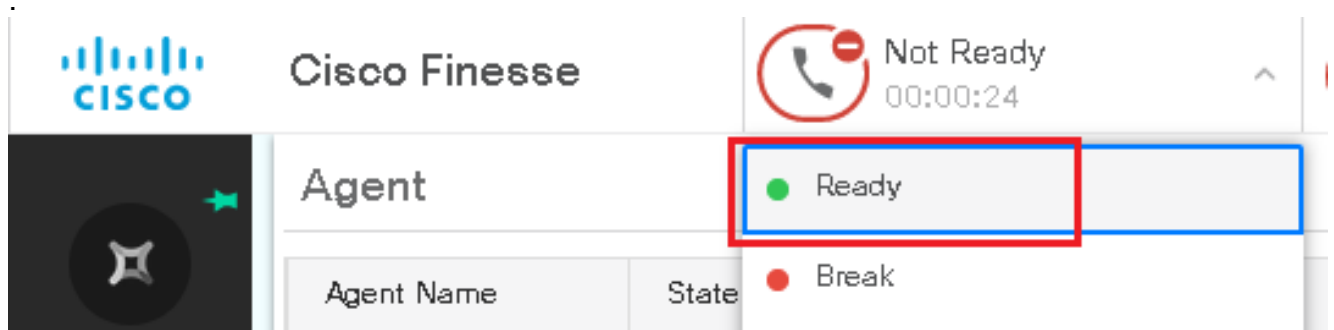
Para validar que RTP está asegurado correctamente, siga estos pasos:

1. Realice una llamada de prueba al centro de contacto y escuche el mensaje de IVR.
2. Al mismo tiempo, abra la sesión SSH en vCUBE y ejecute este comando:
show call active voice brief

```
Total call-legs: 2
1E85 : 100642 465092660ms.1 (02:55:19.809 UTC Thu Mar 25 2021) +1090 pid:6000100 Answer 3227046971 active
dur 00:00:26 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.76:5062 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:4865626844c25f248e19a95a65b0ad50
RemoteUUID:674ECD1639ED7A710000ABF910000178
VRF:
1E85 : 100643 465093670ms.1 (02:55:20.819 UTC Thu Mar 25 2021) +70 pid:6000 Originate 6016 active
dur 00:00:26 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.143:25346 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:674ECD1639ED7A710000ABF910000178
RemoteUUID:4865626844c25f248e19a95a65b0ad50
VRF:
```

Sugerencia: compruebe si el SRTP es on entre CUBE y VVB (198.18.133.143). Si la respuesta es sí, esto confirma que el tráfico RTP entre CUBE y VB es seguro.

3. Hacer que un agente esté disponible para contestar la llamada.

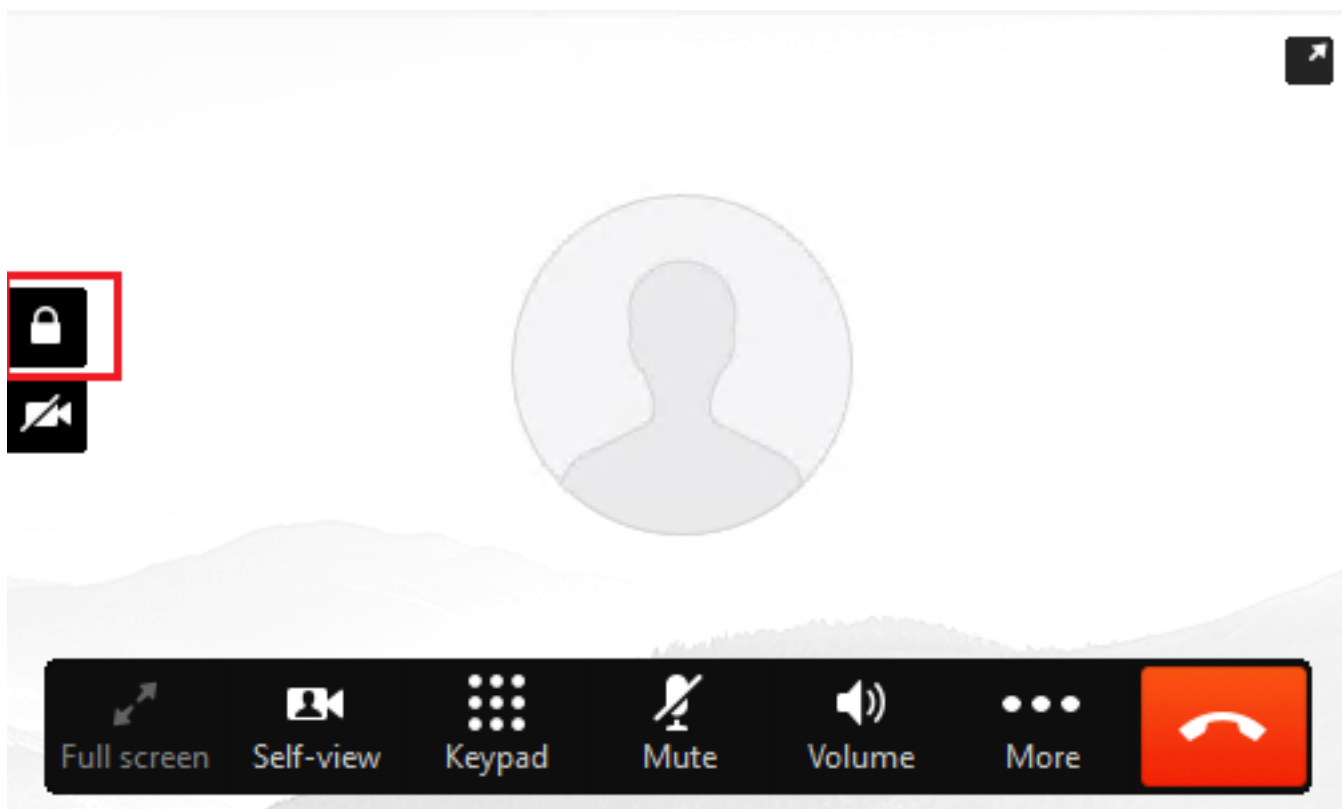


4. El agente se reserva y la llamada se enruta al agente. Conteste la llamada.
5. La llamada se conecta con el agente. Vuelva a la sesión SSH de vCUBE y ejecute este comando:
show call active voice brief

```
Total call-legs: 2
1E85 : 100642 465092660ms.1 (02:55:19.809 UTC Thu Mar 25 2021) +1090 pid:6000100 Answer 3227046971 connected
dur 00:04:01 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.76:5062 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE: Off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:4865626844c25f248e19a95a65b0ad50
RemoteUUID:00003e7000105000a000005056a06cb8
VRF:
1E85 : 100643 465093670ms.1 (02:55:20.819 UTC Thu Mar 25 2021) +70 pid:6000 Originate 6016 connected
dur 00:04:01 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.75:24648 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE: Off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:00003e7000105000a000005056a06cb8
RemoteUUID:4865626844c25f248e19a95a65b0ad50
VRF:
```

Sugerencia: compruebe si el SRTP es on entre CUBE y los teléfonos de los agentes (198.18.133.75). En caso afirmativo, esto confirma que el tráfico RTP entre CUBE y el agente es seguro.

6. Además, una vez conectada la llamada, se muestra un bloqueo de seguridad en el dispositivo del agente. Esto también confirma que el tráfico RTP es seguro.



Para validar que las señales SIP están aseguradas correctamente, consulte el artículo [Configure Secure SIP Signaling](#).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).